ON THE DISTRIBUTION OF CLASS GROUPS OF NUMBER FIELDS

GUNTER MALLE

ABSTRACT. We propose a modification of the predictions of the Cohen–Lenstra heuristic for class groups of number fields in the case where roots of unity are present in the base field. As evidence for this modified formula we provide a large set of computational data which show close agreement. Furthermore, our predicted formula agrees with results on class groups of function fields in positive characteristic for which the base field contains appropriate roots of unity.

1. INTRODUCTION

The distribution of class groups of number fields remains mysterious. The Cohen–Lenstra–philosophy, extended by Cohen–Martinet [6] gives a heuristic approach with very precise predictions which is widely expected to be accurate, but only very few isolated instances have been proved. Recently, though, we presented computational evidence [8] that the Cohen–Lenstra–heuristic fails for the p-part of class groups in the presence of pth roots of unity in the base field. In particular it never seems to apply for the case $p = 2$.

Here, we propose a modified prediction in this case, and present various computational data in support of this new formula.

In Section 3 we compare our prediction with results on class groups of function fields, which are related to the distribution of elements in finite symplectic groups with given eigenspace for the eigenvalue 1.

In order to explain our computational results, let's consider a *situation* $\Sigma := (G, K_0, \sigma)$ consisting of a number field K_0, a transitive permutation group G of degree $n \geq 2$, and a possible signature σ of a degree n extension K/K_0 with Galois group (of the Galois closure) permutation isomorphic to G. For such a situation Σ, let $\mathcal{K}(\Sigma)$ denote the set of degree n extensions K/K_0 of K_0 (inside a fixed algebraic closure of $\mathbb{Q}$) with Galois group G and signature σ. We are interested in the structure of the relative class group $\mathrm{Cl}(K/K_0)$ of K/K_0 for $K \in \mathcal{K}(\Sigma)$ (the kernel in the class group Cl_K of the norm map from K to K_0).

Here we present numerical data for the distribution of p-parts of class groups for the following situations Σ and primes p:

(1) $\Sigma = (C_2, \mathbb{Q}(\sqrt{-3}), \text{complex}), p = 3,$
(2) $\Sigma = (C_2, \mathbb{Q}(\mu_5), \text{complex}), p = 5,$
(3) $\Sigma = (\mathfrak{S}_3, \mathbb{Q}, \text{totally real}), p = 2,$
(4) $\Sigma = (C_3, \mathbb{Q}, \text{totally real}), p = 2,$

(5) $\Sigma = (C_3, \mathbb{Q}(\sqrt{-3}), \text{complex})$, $p = 2$,
(6) $\Sigma = (C_3, \mathbb{Q}(\sqrt{5}), \text{totally real})$, $p = 2$,
(7) $\Sigma = (C_3, \mathbb{Q}(\sqrt{-1}), \text{complex})$, $p = 2$,
(8) $\Sigma = (D_5, \mathbb{Q}, \text{complex})$, $p = 2$,
(9) $\Sigma = (D_5, \mathbb{Q}, \text{real})$, $p = 2$.

2. Class groups in the presence of pth roots of unity

We begin by recalling the setting and the fundamental heuristic assumption in the paper of Cohen and Martinet [6].

Let K_0 be a number field, K_1/K_0 a finite extension, L/K_0 its Galois closure with Galois group $G = \text{Gal}(L/K_0)$. (All number fields here are taken inside a fixed algebraic closure of $\mathbb{Q}$.) Then G acts on the different embeddings of K_1 into L by the transitive permutation representation on its subgroup $\text{Gal}(L/K_1)$. The corresponding permutation character χ contains the trivial character 1_G exactly once, and we let $\chi_1 := \chi - 1_G$. Let $\mathbb{Q}[G]$ denote the rational group ring of the Galois group G. We make the following two assumptions, which will be satisfied in all examples considered:

(1) χ_1 is the character of an irreducible (but not necessarily absolutely irreducible) $\mathbb{Q}[G]$-module,
(2) any absolutely irreducible constituent φ of χ_1 has Schur index 1, that is, φ is the character of a representations of G over the field of values of φ.

Note that (1) implies in particular that $\text{Gal}(L/K_1)$ is a maximal subgroup of G, or equivalently that the extensions K_1/K_0 is simple. We write $\mathcal{O}$ for the ring of integers of the field of values of any absolutely irreducible constituent φ of χ_1. (This is an abelian, hence normal extension of $\mathbb{Q}$, and thus independent of the choice of constituent φ by (1) above.)

Denote by E_L the group of units of the ring of integers of L. Then the action of G makes $E_L \otimes_{\mathbb{Z}} \mathbb{Q}$ into a $\mathbb{Q}[G]$-module, whose character we denote by χ_E. (It can be computed explicitly in terms of the signature σ of L/K_0 by the theorem of Herbrandt, see [6, Th. 6.7].) We set

$$u := \langle \chi_E, \varphi \rangle$$

(see [6, p.63]), the scalar product of the character χ_E with an absolutely irreducible constituent φ of χ_1. Since χ_E is rational, this does not depend on the choice of φ.

Let's denote by $\mathcal{K}(\Sigma)$, where $\Sigma = (G, K_0, \sigma)$, the set of number fields K/K_0 with signature σ and Galois group of the Galois closure permutation isomorphic to G. Note that both the isomorphism type of the $\mathbb{Q}[G]$-module $E_L \otimes \mathbb{Q}$ and the integer u only depend on the situation Σ, not on K_1 or L. We are interested in the distribution of relative class groups of fields in $\mathcal{K}(\Sigma)$.

By the fundamental assumption of [6, Hyp. 6.6] there should be a notion of *good primes* for Σ, including in particular all primes not dividing $|G|$, and maybe even those not dividing the permutation degree of G, such that whenever p is good for Σ and $u \geq 1$, then a given finite p-torsion $\mathcal{O}$-module H should occur as Sylow

p-subgroup of a class group $\mathrm{Cl}(K/K_0)$ for $K \in \mathcal{K}(\Sigma)$ with probability

$$\frac{c}{|H|^u |\mathrm{Aut}_{\mathcal{O}}(H)|}$$

for some constant c only depending on p and Σ (see [6, Th. 5.6(ii)]).

The computational data obtained in [8] indicated that this latter assertion is probably wrong for primes p such that K_0 contains pth roots of unity, that is, such primes are not good for Σ. Based on further and more extensive computations, instead we propose a modified formula at least for the case when no p^2th roots of unity lie in K_0, and $\mathcal{O} = \mathbb{Z}$:

Conjecture 2.1. *Assume that p does not divide the permutation degree of G and that K_0 contains the pth but not the p^2th roots of unity. Then a given finite p-group H of p-rank r occurs as Sylow p-subgroup of a relative class group $\mathrm{Cl}(K/K_0)$ for $K \in \mathcal{K}(\Sigma)$ with probability*

$$c \frac{\prod_{i=1}^{r+u}(p^i - 1)}{p^{r(u+1)}} \cdot \frac{1}{|H|^u |\mathrm{Aut}(H)|} ,$$

where

$$c = \frac{1}{\prod_{i=u+1}^{\infty}(1 + p^{-i})} = \frac{(p^2)_u (p)_\infty}{(p)_u (p^2)_\infty}$$

and $u = u(\Sigma)$ is as introduced above.

Here, for $q, k \in \mathbb{N}$ we let

$$(q)_k := \prod_{i=1}^{k}(1 - q^{-i}), \qquad (q)_\infty := \prod_{i=1}^{\infty}(1 - q^{-i}).$$

Proposition 2.2. *Assume that the Sylow p-subgroups of class groups $\mathrm{Cl}(K/K_0)$ for $K \in \mathcal{K}(\Sigma)$ are distributed according to Conjecture 2.1. Then the probability that $\mathrm{Cl}(K/K_0)$ has p-rank equal to r is given by*

$$\mathrm{pr}(\mathrm{rnk}_p(\mathrm{Cl}(K/K_0)) = r) = \frac{(p^2)_u (p)_\infty}{(p)_u (p^2)_\infty} \cdot \frac{1}{p^{r(r+2u+1)/2}(p)_r}$$

with nth higher moments

$$\prod_{k=1}^{n}(1 + p^{k-u-1}) \qquad (n \in \mathbb{N}).$$

Proof. This follows easily as in [8, Lemma 2.1 and 2.2]. $\qquad\square$

Computationally, only very few cases with $\mathcal{O} \neq \mathbb{Z}$ are in reach. The data obtained there seem to indicate the following generalization of the above formula: Assume that p is good for Σ and that K_0 contains the pth but not the p^2th roots of unity. Then a given finite p-torsion $\mathcal{O}$-module H of $\mathcal{O}$-rank r should occur as Sylow p-subgroup of a class group with probability

(2.1) $$c \frac{d^r \prod_{i=1}^{r+u}(q^i - 1)}{q^{r(u+1)}} \cdot \frac{1}{|H|^u |\mathrm{Aut}_{\mathcal{O}}(H)|}$$

for some constant c only depending on p and Σ, where $q := |\mathcal{O}/p\mathcal{O}|$ and $d = (\mathcal{O} : \mathbb{Z})$.

Computations for cases where the base field contains the p^2th roots of unity, for example on the 2-parts of class groups of cubic extensions of the field of fourth roots of unity (see Section 6.4), or on the 3-parts of class groups of quadratic extensions of the field of ninth roots of unity, show that while the distribution of p-ranks might still be given as in Proposition 2.2 the distribution of Sylow p-subgroups seems to be different from the formula given in Conjecture 2.1. We hope to come back to this question in some future investigation.

In Sections 4–7, we consider several instances of situations Σ, for which we specialize the conjecture and give supporting computational data.

3. Relation with class groups of function fields

First, we compare our new formula to results and heuristics for class groups of global fields in positive characteristic, that is, function fields over finite fields $\mathbb{F}$. Here, the base field contains pth roots of unity if p divides $|\mathbb{F}| - 1$. Now for a prime power q and for $g, r \geq 0$, let

$$\alpha_q(g, r) := \frac{|\{x \in \mathrm{Sp}_{2g}(q) \mid \dim(\ker(x - \mathrm{id})) = r\}|}{|\mathrm{Sp}_{2g}(q)|},$$

where $\mathrm{Sp}_{2g}(q)$ denotes the symplectic group of dimension $2g$ over $\mathbb{F}_q$. In [1, Thm. 3.1] Achter proves that the probability for the class group of a function field over $\mathbb{F}$ of genus g to have p-rank r converges to $\alpha_q(g, r)$ as $|\mathbb{F}| \to \infty$ with p dividing $|\mathbb{F}| - 1$ (see also [2, Thm. 3.1]). Achter [1, Lemma 2.4] shows that $\alpha_q(g, r)$ has a limit for $g \to \infty$. Here we give an explicit values for this limit, using the explicit formulas for $\alpha_q(g, r)$ which were obtained by Rudvalis and Shinoda, see [7, Cor. 1]:

Proposition 3.1. *For any prime power q, and $r \geq 0$ we have*

$$\lim_{g \to \infty} \alpha_q(g, r) = \frac{(q)_\infty}{(q^2)_\infty} \cdot \frac{1}{q^{r(r+1)/2}(q)_r}.$$

Thus, the distribution of elements in $\mathrm{Sp}_{2g}(p)$ according to the dimension of their eigenspace for the eigenvalue 1 converges to the conjectured distribution of p-ranks of class groups in Proposition 2.2 for unit rank $u = 0$.

Proof. First assume that $r = 2k$ is even. By [7, Cor. 1] and using

$$|\mathrm{Sp}_{2k}(q)| = q^{k^2} \prod_{i=1}^{k} (q^{2i} - 1)$$

we have

$$\alpha_q(g, 2k) = \frac{1}{|\mathrm{Sp}_{2k}(q)|} \sum_{i=0}^{g-k} \frac{(-1)^i q^{i(i+1)}}{|\mathrm{Sp}_{2i}(q)| q^{2ik}}$$

$$= \frac{1}{|\mathrm{Sp}_{2k}(q)|} \sum_{i=0}^{g-k} \frac{(-1)^i q^{-i^2-2ik}}{(1 - q^{-2}) \cdots (1 - q^{-2i})}$$

$$= \frac{1}{|\mathrm{Sp}_{2k}(q)|} \left(1 + \sum_{i=1}^{g-k} \frac{(q^2)^{-\binom{i}{2}} (-q)^{i(2k+1)}}{(1 - q^{-2}) \cdots (1 - q^{-2i})} \right).$$

(Note that the exponent $\binom{i}{2}$ at q^2 in the numerator in loc. cit. should correctly read $\binom{i+1}{2}$.) For $g \to \infty$, the latter converges to

$$\frac{1}{|\mathrm{Sp}_{2k}(q)|} \prod_{i=k}^{\infty} (1 - q^{-2i-1})$$

by [3, Cor. 2.2]. A trivial rewriting gives the value stated in the conclusion.

For odd $r = 2k + 1$ we have

$$\alpha_q(g, 2k+1) = \frac{1}{q^{2k+1} |\mathrm{Sp}_{2k}(q)|} \sum_{i=0}^{g-k-1} \frac{(-1)^i q^{i(i+1)}}{|\mathrm{Sp}_{2i}(q)| q^{2i(k+1)}}$$

by [7, Cor. 1] (again with the corrected power of q in the numerator), so by a completely analogous calculation we find

$$\lim_{g \to \infty} \alpha_q(g, r) = \frac{1}{q^{2k+1} |\mathrm{Sp}_{2k}(q)|} \prod_{i=k+1}^{\infty} (1 - q^{-2i-1})$$

from which the claim follows easily. □

It seems tempting to speculate that even the distribution of class groups in the number field case is as given in [1, 2] for the corresponding function field case in the presence of roots of unity. We have not (yet) been able to match that with our Conjecture 2.1.

4. Quadratic extensions and odd primes p

We now turn to experimental evidence for Conjecture 2.1. Our first set of examples concerns the p-part of class groups of quadratic extensions of a number field containing the pth roots of unity, where $p = 3$ or $p = 5$. Here, in the notation of the previous section $G = Z_2$ is of order 2, and $\chi_1 = \mathrm{sgn}$ is its non-trivial linear character, the sign character of $\mathfrak{S}_2 = Z_2$.

4.1. **Quadratic extensions of $\mathbb{Q}(\sqrt{-3})$.** The smallest such situation occurs for quadratic extensions of the field $K_0 := \mathbb{Q}(\sqrt{-3})$ of third roots of unity. Here, K_0 has a unique place at infinity, and Herbrandt's formula gives $\chi_E = \mathrm{sgn}$, so $u = 1$. The prime $p = 3$ is good for this situation, but since the third roots of unity are present, we expect the Cohen–Lenstra–Martinet heuristic to fail. In [8, (3)] we

already proposed that the distribution of 3-ranks r of class groups should be given by

$$(4.1) \qquad \mathrm{pr}(\mathrm{rnk}_3(\mathrm{Cl}_K) = r) = \frac{4}{3} \cdot \frac{(3)_\infty}{(9)_\infty} \cdot \frac{1}{3^{r(r+3)/2}(3)_r}$$

with higher moments

$$\prod_{k=1}^{n}(1 + 3^{k-2})$$

(see Proposition 2.2). According to Cohen et al. [4, Cor. 1.3] asymptotically the number of quadratic extensions of K_0 of discriminant at most X grows linearly with X, with proportionality factor 0.02613532018111.... Those extensions which are Galois over $\mathbb{Q}$ have density 0, so generically, the Galois closure over $\mathbb{Q}$ has dihedral Galois group D_4 of order 8. In particular, generically the quadratic extensions come in pairs with the same Galois closure over $\mathbb{Q}$. So we expect to find roughly $0.01306766\, X$ quartic extensions of $\mathbb{Q}$ with intermediate field K_0 and of discriminant at most X.

Extending the data presented in [8, Tab. 9] we have compiled lists S consisting of the first $|S|$ quadratic extensions of K_0 of discriminant at least D, for various values of D. The numbers of fields obtained are in very close accordance with the asymptotic formula derived above. In Table 1 we give the results of our computations of 3-ranks for these fields. Visibly, the data fit the prediction in (4.1) quite closely.

TABLE 1. C_2-fields over $\mathbb{Q}(\sqrt{-3})$: 3-ranks and higher moments

D	$|S|$	$r = 0$	1	2	3	$n = 1$	2	3
$\geq 10^{16}$	$2 \cdot 10^6$	.8528	.141	.0058	.71E–4	1.331	2.648	10.55
$\geq 10^{20}$	$4 \cdot 10^6$	.8521	.142	.0059	.68E–4	1.333	2.656	10.43
$\geq 10^{24}$	$2 \cdot 10^5$	.8525	.142	.0057	.80E–4	1.331	2.650	10.43
formula (4.1)		.8520	.142	.0059	.76E–4	1.333	2.667	10.67
CL-prediction		.8402	.158	.0023	.33E–5	1.333	2.444	6.81

Conjecture 2.1 now predicts more precisely that a 3-group H of 3-rank r occurs as Sylow 3-subgroup of a class group of a quadratic extension of $\mathbb{Q}(\sqrt{-3})$ with probability

$$(4.2) \qquad 2 \cdot \frac{(3)_\infty}{(9)_\infty} \cdot \frac{3^{(r^2-r)/2}(3)_{r+1}}{|H| \cdot |\mathrm{Aut}(H)|}$$

while the original Cohen–Lenstra–Martinet heuristic [5, 6] predicts a relative frequency of

$$\frac{(3)_\infty}{(3)_1} \cdot \frac{1}{|H| \cdot |\mathrm{Aut}(H)|}.$$

The following Table 2 contains detailed statistics for the Sylow 3-subgroups for the same sets of data as in Table 1 by giving the quotient of the actual number of fields with given Sylow 3-subgroup divided by the number expected according to formula (4.2).

The last line of Table 2 lists the proportion predicted by (4.2).

TABLE 2. C_2-fields over $\mathbb{Q}(\sqrt{-3})$: Sylow 3-subgroups

D	1	3	9	3^2	27	9×3	81	27×3	3^3
$\geq 10^{16}$	1.0009	.995	.998	.981	.991	.944	.985	.954	.873
$\geq 10^{20}$	1.0001	1.000	.997	.989	1.016	1.009	.999	.942	.858
$\geq 10^{24}$	1.0006	.998	1.001	.983	.943	.913	.924	.720	1.248
eq. (4.2)	.852	.126	.014	.0051	.0016	.75E–3	.17E–3	.83E–4	.64E–4

The table shows a remarkably good agreement with our prediction.

4.2. Quadratic extensions of $\mathbb{Q}(\sqrt{5})$ and of $\mathbb{Q}(\sqrt{-1})$.

We have computed similar data as above for totally real quadratic extensions of $\mathbb{Q}(\sqrt{5})$, resp. of quadratic extensions of $\mathbb{Q}(\sqrt{-1})$. Here, according to [4, Cor. 1.3] the number of expected fields (over $\mathbb{Q}$) of discriminant at most X should grow linearly, with proportionality factor 0.001852542... respectively 0.008144834.... In these situations, K_0 does not contain the third roots of unity. Our results for $p = 3$-parts of class groups are in close agreement with the Cohen–Lenstra–Martinet prediction, so we don't show the details.

4.3. Quadratic extensions of $\mathbb{Q}(\mu_5)$.

Our final set of examples in this section consists of quadratic extensions of the field $K_0 := \mathbb{Q}(\mu_5)$ of fifth roots of unity. Here, we expect the prime $p = 5$ to behave differently. The base field has two places at infinity, so $\chi_E = 1 + 2\,\mathrm{sgn}$ and $u = 2$. According to Conjecture 2.1 a 5-group H of 5-rank r occurs as Sylow 5-subgroup of a class group of a quadratic extension of $\mathbb{Q}(\mu_5)$ with probability

$$(4.3) \qquad \frac{13}{8} \frac{(5)_\infty}{(25)_\infty} \frac{5^{(r^2-r)/2}(5)_{r+2}}{|H|^2\,|\mathrm{Aut}(H)|}.$$

Thus, by Proposition 2.2 the distribution of 5-ranks should be given by

$$(4.4) \qquad \mathrm{pr}(\mathrm{rnk}_5(\mathrm{Cl}_K) = r) = \frac{156}{125} \cdot \frac{(5)_\infty}{(25)_\infty} \cdot \frac{1}{5^{r(r+5)/2}(5)_r}$$

with higher moments

$$\prod_{k=1}^{n}(1 + 5^{k-3}), \qquad n = 1, 2, \ldots.$$

We have compiled lists S of the first 10^5 such extensions of discriminant $D \geq 10^i$, $i = 14, 18, 22$. Again by [4, Cor. 1.3], the number of such fields (over $\mathbb{Q}$) of discriminant at most X should equal roughly

$$0.12444267\ldots \cdot 10^{-5}\,X,$$

which agrees closely with the numbers obtained here. Table 3 shows the distribution of 5-ranks for these sets of fields, together with old and new prediction. The predictions for rank 0 and rank 1 are very close together, but according to (4.4), rank 2

should occur about five times more frequently than for the original prediction, which fits with the data.

TABLE 3. C_2-fields over $\mathbb{Q}(\mu_5)$: 5-ranks and higher moments

D	$|S|$	$r = 0$	1	2	$n = 1$	2	3
$\geq 10^{14}$	10^5	.99089	.91E–2	.10E–4	1.0366	1.2246	2.285
$\geq 10^{18}$	10^5	.99052	.95E–2	.10E–4	1.0381	1.2335	2.330
$\geq 10^{22}$	10^5	.98987	1.01E–2	.10E–4	1.0407	1.2491	2.411
formula (4.4)		.99008	.99E–2	.16E–4	1.0400	1.2480	2.496
CL-prediction		.99002	1.00E–2	.33E–5	1.0400	1.2416	2.290

The amount of data computed in this case is not sufficient to obtain reliable results on the distribution of Sylow subgroups, so these are not shown.

5. Non-Galois cubic fields

A further interesting situation for our conjecture occurs for non-Galois cubic extensions of $\mathbb{Q}$ with the prime $p = 2$.

5.1. Totally real non-Galois cubic fields.
The number of totally real $\mathfrak{S}_3$-fields of discriminant at most X is expected to behave asymptotically as

$$c_1 X - c_2 \frac{1}{\sqrt{3}+1} X^{5/6} + o(X^{1/2})$$

where

$$c_1 = 0.06932561438172562..., \qquad c_2 = 0.403483636663946799...$$

(see Roberts [9, Conj. 3.1]). We have computed the first 10^6 such fields of discriminant at least 10^i, where $11 \leq i \leq 17$. Table 4 compares the actual number of $\mathfrak{S}_3$-fields of discriminant D between $D_1 \leq D \leq D_2$ with the number predicted by the asymptotic formula.

TABLE 4. Totally real $\mathfrak{S}_3$-fields: asymptotic vs. actual numbers

D_1	D_2	$|S|$	expected
10^{11}	$10^{11} + 14816837$	10^6	1 000 421
10^{12}	$10^{12} + 14672596$	10^6	999 129
10^{13}	$10^{13} + 14613109$	10^6	1 000 810
10^{14}	$10^{14} + 14544488$	10^6	999 997
10^{15}	$10^{15} + 14467409$	10^6	997 331
10^{16}	$10^{16} + 14496840$	10^6	1 001 158
10^{17}	$10^{17} + 14464985$	10^6	1 000 181

For the totally real case the theorem of Herbrandt gives $u = 2$. So Proposition 2.2 predicts the distribution

$$(5.1) \qquad \mathrm{pr}(\mathrm{rnk}_2(\mathrm{Cl}_K) = r) = \frac{15}{8} \cdot \frac{(2)_\infty}{(4)_\infty} \cdot \frac{1}{2^{r(r+5)/2}(2)_r}$$

for the 2-ranks of class groups, with higher moments

$$\prod_{k=1}^{n}(1 + 2^{k-3}), \qquad n = 1, 2, \ldots$$

(this was already proposed in our previous paper [8, (5)]). Computational data for this case which reach considerably farther than those in [8, Table 10] are displayed in Table 5.

TABLE 5. Totally real $\mathfrak{S}_3$-fields: 2-ranks and higher moments

D	$|S|$	$r = 0$	1	2	3	$n = 1$	2	3	4
$\geq 10^{12}$	10^6	.798	.188	.0135	.354E–3	1.231	1.79	3.35	8.72
$\geq 10^{14}$	10^6	.793	.192	.0149	.431E–3	1.240	1.83	3.53	9.84
$\geq 10^{16}$	10^6	.789	.195	.0157	.507E–3	1.246	1.85	3.64	10.47
$\geq 10^{17}$	10^6	.788	.195	.0158	.538E–3	1.247	1.86	3.68	10.76
formula (5.1)		.786	.197	.0164	.585E–3	1.250	1.87	3.75	11.25
CL-prediction		.770	.220	.0098	.090E–3	1.250	1.81	3.20	7.18

Conjecture 2.1 predicts that a 2-group H of 2-rank r occurs as Sylow 2-subgroup of a class group of a totally real non-Galois cubic number field with probability

$$(5.2) \qquad 5 \cdot \frac{(2)_\infty}{(4)_\infty} \cdot \frac{2^{(r^2-r)/2}(2)_{r+2}}{|H|^2 \cdot |\mathrm{Aut}(H)|}.$$

As evidence for this we give in Table 6 the quotient of the actual number of fields with given Sylow 2-subgroup divided by the number expected according to formula (5.2). In addition, in the last two lines we print the relative frequency according to (5.2) and according to the the original Cohen–Lenstra heuristic.

TABLE 6. Totally real $\mathfrak{S}_3$-fields: Sylow 2-subgroups

D	1	2	4	2^2	8	4×2	2^3	16	8×2	4^2
$\geq 10^{10}$	1.032	.905	.885	.670	.883	.667	.32	.85	.70	.57
$\geq 10^{12}$	1.015	.956	.955	.829	.927	.814	.62	.91	.79	.80
$\geq 10^{14}$	1.008	.975	.983	.917	.969	.885	.72	1.05	.88	.78
$\geq 10^{16}$	1.003	.990	1.008	.964	1.009	.954	.87	.97	.86	.95
$\geq 10^{17}$	1.002	.993	.997	.958	1.001	.994	.89	.95	1.04	.91
eq. (5.2)	.852	.126	.014	.0051	.0016	.75E–3	.17E–3	.8E–4	.6E–4	.2E–4
[5]	.840	.140	.016	.0019	.0017	.29E–3	.19E–3	.3E–4	.3E–5	.2E–5

The table shows a reasonably good agreement with our prediction.

6. Cyclic cubic fields

Our third set of examples concerns Sylow 2-subgroups of cyclic cubic fields over various base fields. Here $G = Z_3$ is of order 3, $\mathcal{O} = \mathbb{Z}[\mu_3]$ and χ_1 is the sum of the two non-rational linear characters of G.

6.1. **Cyclic cubic fields over** $\mathbb{Q}$**.** The smallest situation, where $K_0 = \mathbb{Q}$, was already considered in [8, Sec. 2], where extensive computational results for 2-ranks of class groups were presented. Here $u = 1$, so according to Proposition 2.2 the 2-ranks of class groups should be distributed according to

$$(6.1) \qquad \mathrm{pr}(\mathrm{rnk}_2(\mathrm{Cl}_K) = 2r) = \frac{3}{2} \cdot \frac{(2)_\infty (16)_\infty}{(4)_\infty^2} \cdot \frac{1}{2^{r(r+2)}(4)_r}$$

(see [8, (1)]), while a given 2-torsion $\mathcal{O}$-module H of (even) 2-rank $2r$ should occur with probability

$$(6.2) \qquad 2\frac{(2)_\infty (16)_\infty}{(4)_\infty^2} \cdot \frac{2^{r^2}(4)_{r+1}}{|H| \cdot |\mathrm{Aut}_\mathcal{O}(H)|}$$

as Sylow 2-subgroup of a class group of a cyclic cubic number. As evidence for this, we list in Table 7 the relative proportions of certain 2-groups as Sylow 2-subgroups of class groups of C_3-fields. Also, in Table 8 we give the corresponding results for fields of prime conductor. The predicted values for some small 2-groups are given in the last line of Tables 7 and 8 respectively (see also [5, 2(a)]).

TABLE 7. C_3-fields: Sylow 2-subgroups

D	$|S|$	1	2^2	4^2	2^4	8^2	$4^2 \times 2^2$	2^6	16^2
$\geq 10^{20}$	10^5	1.003	.988	1.010	.878	.749	.995	.578	1.23
$\geq 10^{22}$	10^5	1.000	.999	.994	.969	.999	1.288	.868	.61
$\geq 10^{24}$	10^5	1.001	.989	1.067	1.063	.749	1.054	1.157	.31
$\geq 10^{26}$	10^5	1.000	1.002	.996	.963	.960	1.024	.868	1.84
eq. (6.2)		.853	.133	.0083	.0044	.52E–3	.34E–3	.35E–4	.33E–4
[5]		.918	.076	.0048	.0003	.30E–3	.25E–4	.79E–7	.19E–4

TABLE 8. C_3-fields of prime conductor: Sylow 2-subgroups

D	$|S|$	1	2^2	4^2	2^4	8^2	$4^2 \times 2^2$	2^6	16^2
$\geq 10^{22}$	$6 \cdot 10^6$	1.001	.997	.999	.988	.980	1.005	1.051	.96
$\geq 10^{28}$	10^6	1.000	1.002	1.004	.979	1.074	.954	1.186	1.26
$\geq 10^{32}$	10^5	1.000	1.003	.992	.983	.980	.790	.868	.61

6.2. **Cyclic cubic extensions of** $\mathbb{Q}(\sqrt{-3})$**.** As a second case we have investigated cyclic cubic extensions of the complex quadratic number field $K_0 = \mathbb{Q}(\sqrt{-3})$. Here, again $u = 1$, so according to Conjecture 2.1 a given 2-torsion $\mathcal{O}$-module H of 2-rank $2r$ should occur with the same probability (6.2) as in the previous case. Table 9 gives results on this case by listing the quotient of the observed densities by the predicted density, for sets of 10^5 fields of discriminant at least 10^i, for $i \in \{16, 20, 24\}$. Again, the data seem in agreement with our conjecture.

TABLE 9. C_3-fields over $\mathbb{Q}(\sqrt{-3})$: Sylow 2-subgroups

D	$\|S\|$	1	2^2	4^2	2^4	8^2	$4^2 \times 2^2$	2^6	16^2
$\leq 10^{14}$	499 815	1.034	.820	.817	.307	.815	.316	0	.615
$\geq 10^{16}$	10^5	1.018	.901	.951	.546	.999	.732	0	.307
$\geq 10^{20}$	10^5	1.007	.967	.965	.780	.922	.732	1.157	.921
$\geq 10^{24}$	10^5	1.002	.991	.987	.949	.922	.966	1.157	.615
eq. (6.2)		.853	.133	.0083	.0044	.52E–3	.34E–3	.35E–4	.33E–4

6.3. **Cyclic cubic extensions of $\mathbb{Q}(\sqrt{5})$.** In the case of a real quadratic base field K_0 we have $u = 2$, so Proposition 2.2 predicts the distribution

$$(6.3) \qquad \mathrm{pr}(\mathrm{rnk}_2(\mathrm{Cl}_K) = 2r) = \frac{27}{16} \cdot \frac{(2)_\infty (16)_\infty}{(4)_\infty^2} \cdot \frac{1}{2^{r(r+4)}(4)_r}$$

for the 2-ranks of class groups, with higher moments

$$\prod_{k=1}^{n}(1 + 2^{2k-5}).$$

More precisely, Conjecture 2.1 predicts that a 2-torsion $\mathcal{O}$-module H of 2-rank $2r$ should occur with probability

$$(6.4) \qquad \frac{12}{5} \cdot \frac{(2)_\infty (16)_\infty}{(4)_\infty^2} \cdot \frac{2^{r^2}(4)_{r+2}}{|H|^2 \cdot |\mathrm{Aut}_\mathcal{O}(H)|}$$

as Sylow 2-subgroup of a class group of a cyclic cubic number. Data for the case $K_0 = \mathbb{Q}(\sqrt{5})$ are listed in Tables 10 and 11.

TABLE 10. C_3-fields over $\mathbb{Q}(\sqrt{5})$: 2-ranks and higher moments

D	$\|S\|$	$r = 0$	2	4	$n = 1$	2	3	4
$\leq 10^{16}$	236 832	.9672	.0327	.11E–3	1.100	1.518	3.51	16.5
$\geq 10^{20}$	10^5	.9627	.0370	.30E–3	1.115	1.631	4.56	30.1
$\geq 10^{24}$	10^5	.9596	.0401	.27E–3	1.124	1.670	4.63	28.9
$\geq 10^{28}$	10^5	.9594	.0402	.34E–3	1.126	1.690	4.93	33.5
eq. (6.3)		.9597	.0400	.33E–3	1.125	1.687	5.06	45.6
CL-prediction		.9793	.0207	.02E–3	1.062	1.316	2.39	7.7

TABLE 11. C_3-fields over $\mathbb{Q}(\sqrt{5})$: Sylow 2-subgroups

D	1	2^2	4^2	2^4	8^2	$4^2 \times 2^2$	2^6
$\leq 10^{16}$	1.008	.816	.906	.336	1.318	0	0
$\geq 10^{20}$	1.003	.923	1.073	.918	0	0	0
$\geq 10^{24}$	1.000	1.003	1.008	.826	2.081	0	0
$\geq 10^{28}$	1.000	1.005	1.089	1.010	2.081	1.567	0
eq. (6.4)	.960	.039	.61E–3	.33E–3	.96E–5	.64E–5	.65E–6

6.4. **Cyclic cubic extensions of** $\mathbb{Q}(\sqrt{-1})$**.** Now we choose the base field $K_0 = \mathbb{Q}(\sqrt{-1})$ containing the 4th roots of unity. The relevant unit rank equals $u = 1$. This situation is not covered by the predictions made in Section 2. Still, the data in Table 12 seems to confirm that the 2-ranks behave according to formula (6.1). On the other hand, the distribution of individual Sylow 2-subgroups shown in Table 13 does *not* seem to follow the formulas from (6.2).

TABLE 12. C_3-fields over $\mathbb{Q}(\sqrt{-1})$: 2-ranks and higher moments

D	$|S|$	$r = 0$	2	4	6	$n = 1$	2	3	4
$\leq 10^{15}$	$227\,756$	.8642	.1327	.303E–2	0	1.444	3.76	21.7	233
$\geq 10^{20}$	$5 \cdot 10^5$	.8555	.1403	.419E–2	.1E–4	1.485	4.23	30.7	546
$\geq 10^{24}$	$5 \cdot 10^5$	.8541	.1412	.470E–2	.2E–4	1.496	4.42	35.4	747
$\geq 10^{28}$	$5 \cdot 10^5$	.8533	.1419	.473E–2	.5E–4	1.499	4.52	41.4	1119
$\geq 10^{32}$	$4 \cdot 10^5$	.8527	.1425	.472E–2	.5E–4	1.502	4.56	43.1	1227
eq. (6.1)		.8530	.1422	.474E–2	.4E–4	1.500	4.50	40.5	1336

TABLE 13. C_3-fields over $\mathbb{Q}(\sqrt{-1})$: Sylow 2-subgroups

D	1	2^2	4^2	2^4	8^2	$4^2 \times 2^2$	2^6	16^2	$8^2 \times 2^2$
$\leq 10^{15}$	.864	.115	.016	.25E–2	.12E–2	.50E–3	0	.7E–4	.6E–4
$\geq 10^{16}$	.859	.120	.016	.30E–2	.13E–2	.42E–3	0	.2E–3	.4E–4
$\geq 10^{24}$	.854	.123	.017	.40E–2	.11E–2	.64E–3	.1E–4	.7E–4	.3E–4
$\geq 10^{32}$	.853	.125	.017	.40E–2	.10E–2	.62E–3	.4E–4	.6E–4	.4E–4
eq. (6.2)	.853	.133	.0083	.44E–2	.52E–3	.34E–3	.35E–4	.33E–4	.21E–4
[5]	.918	.076	.0048	.03E–2	.30E–3	.25E–4	.79E–7	.19E–4	.16E–4

7. D_5-EXTENSIONS OF $\mathbb{Q}$

The fourth test case consists of quintic extensions of $\mathbb{Q}$ with dihedral Galois group $G = D_5$. Here, $\mathcal{O} = \mathbb{Q}(\sqrt{5})$ and χ_1 is the sum of the two non-rational characters of G of degree 2. Again, the behaviour of the prime $p = 2$ is interesting.

Here, in contrast to the previous cases we don't have a fast method to enumerate *all* D_5-fields between given discriminant bounds nor is there a proven asymptotic formula for the number of such fields. Nevertheless, assuming the Cohen–Lenstra heuristic for the 5-rank of quadratic fields, an obvious asymptotic lower bound for the number of fields is obtained by just counting those fields whose Galois closure is unramified over the quadratic subfield. According to this, for large X there should exist at least $0.07599\sqrt{X}$ complex quintic D_5-fields of discriminant at most X, and at least $0.01507\sqrt{X}$ totally real ones.

We have produced large sets of fields by specializing the D_5-polynomial

$$X^5 - 2\,vX^4 - u(5u^2 - 10uv + 4v^2)X^2 + 2u^2(5u - 4v)(u - v)X$$
$$- 4u^3(u - v)^2 - X^2(X - u)t \ \in \mathbb{Q}(u, v, t)[X]$$

for integral $|u|, |v| \leq 2500$ with $\gcd(u, v) = 1$, and $|t| \leq 50000$. Of these several billion fields, in both possible signatures we retained the first 200,000 ones of discriminant at least 10^i, where $15 \leq i \leq 21$. A priori there is no reason why the class groups of the fields obtained in this way should show the same behaviour as class groups of random D_5-fields. Thus our tables here should be taken with even more care than those in the previous examples.

7.1. Non-real D_5-extensions of $\mathbb{Q}$.

For complex D_5-extensions we obtain $u = 1$, so according to Conjecture 2.1 the (necessarily even) 2-ranks of class groups should be distributed according to the probability in formula (6.1), that is to say, as in the case of cyclic cubic fields.

Despite the fact that our lists of fields are not complete, it turns out that the distributions of 2-ranks given in Table 14 is not too far away from the prediction (6.1).

TABLE 14. Non-real D_5-fields over $\mathbb{Q}$: 2-ranks and higher moments

D	$|S|$	$r = 0$	2	4	6	$n = 1$	2	3
$\leq 10^{15}$	1 183 056	.9266	.0724	.097E–2	.8E–6	1.232	2.34	9.7
$\geq 10^{17}$	200 000	.9110	.0869	.216E–2	.05E–4	1.293	2.87	16.6
$\geq 10^{19}$	200 000	.9049	.0922	.290E–2	.55E–4	1.324	3.35	33.1
$\geq 10^{21}$	200 000	.8992	.0972	.354E–2	.20E–4	1.346	3.46	28.2
eq. (6.1)		.8530	.1422	.474E–2	.38E–4	1.5	4.5	40.5

7.2. Totally real D_5-extensions of $\mathbb{Q}$.

For totally real D_5-extensions we obtain $u = 2$, so according to Conjecture 2.1 the 2-ranks of class groups should be distributed according to formula (6.3).

TABLE 15. Totally real D_5-fields over $\mathbb{Q}$: 2-ranks and higher moments

D	$|S|$	$r = 0$	2	4	6	$n = 1$	2	3
$\leq 10^{14}$	147 683	.9876	.0124	.14E–4	0	1.037	1.19	1.84
$\geq 10^{17}$	200 000	.9789	.0210	.85E–4	0	1.064	1.34	2.67
$\geq 10^{21}$	200 000	.9721	.0276	.19E–3	0	1.086	1.46	3.54
eq. (6.3)		.9597	.0400	.33E–3	.66E–6	1.125	1.69	5.06

REFERENCES

[1] J. ACHTER, The distribution of class groups of function fields. J. Pure Appl. Algebra **204** (2006), 316–333.

[2] J. ACHTER, Results of Cohen-Lenstra type for quadratic function fields. Pp. 1–7 in: *Computational arithmetic geometry*, Contemp. Math., 463, Amer. Math. Soc., Providence, RI, 2008.

[3] G. E. ANDREWS, *The theory of partitions.* Encyclopedia of Mathematics and its Applications, Vol. 2. Addison-Wesley, Reading, 1976.

[4] H. COHEN, F. DIAZ Y DIAZ, M. OLIVIER, On the density of discriminants of cyclic extensions of prime degree. J. Reine Angew. Math. **550** (2002), 169–209.

[5] H. COHEN, J. MARTINET, Class groups of number fields: numerical heuristics. Math. Comp. **48** (1987), 123–137.

[6] H. COHEN, J. MARTINET, Étude heuristique des groupes de classes des corps de nombres. J. Reine Angew. Math. **404** (1990), 39–76.

[7] J. FULMAN, A probabilistic approach to conjugacy classes in the finite symplectic and orthogonal groups. J. Algebra **234** (2000), 207–224.

[8] G. MALLE, Cohen–Lenstra heuristic and roots of unity. J. Number Theory **128** (2008), 2823–2835.

[9] D. ROBERTS, Density of cubic field discriminants. Math. Comp. **70** (2001), 1699–1705.

FB MATHEMATIK, UNIVERSITÄT KAISERSLAUTERN, POSTFACH 3049, D–67653 KAISERSLAUTERN, GERMANY.

E-mail address: `malle@mathematik.uni-kl.de`